IN THE SPECIFICATION

Please amend the second paragraph of page 7 as indicated below.

A1

Figure 2 illustrates one embodiment of the present invention or secured wireless roaming system (hereinafter SWRS) 200. SWRS 200 comprises one or more specially configured wireless stations, such as wireless station 202, at least two specially configured access points, such as access points 206 and 208 and authentication server 210. Access points 206 and 208 are coupled to authentication server 210 via wired network 212 and are further coupled to wireless station 202 via wireless network 204. Authentication server 212 is responsible for maintaining and providing security information and safeguarding the integrity of wired network 212 and wireless network 204. The interactions among access points 206 and 208, wireless station 202 and authentication server ~~212~~ 210 for creating a secured roaming environment will be discussed with examples in the subsequent section that details the operations of SWRS 200.

Please amend the second and the last paragraphs of page 10 as indicated blow.

A2

In conjunction with Figures 2 and 3, instead of acting like a Kerberos client as in a typical application of the Kerberos protocol, authentication protocol engine 316 instructs wireless station 202 to behave as a Kerberos server and provides access point 208 with its identity information in block 400. Then authentication protocol engine 316 waits to respond to access point 206's attempt to establish a secured session using the newly obtained session_key$_{206}$ in block 402. A session is considered secured when wireless station 202 and access point 206 complete their mutual authentication within the lifetime of session_key$_{206}$. After authentication protocol engine 316 confirms that a secured session has been established in block 404, wireless station 202 obtains ID$_g$

from access point 206 in block 406. ID$_g$ enables wireless station 202 to access all the access points that share the same ID$_g$, such as access point 208.

A2

However, wireless station 202 cannot proceed to establish a secured session with access point 208 unless it has another valid session key, or session_key$_{208}$. As wireless station 202 moves into the coverage area of access point 208, authentication protocol engine 316 switches wireless station 202's role back to being a Kerberos client and requests for session_key$_{208}$ from authentication server 210 in block 408. It is important to note that in a typical application of the Kerberos protocol, a Kerberos client needs to have the identity information of a peer system prior to initiating a session with such a system. In contrast, one embodiment of wireless station 202 simply uses session_key$_{208}$ and ID$_g$ to initiate a session with access point 208 in block 410.